[illegible]

www.huawei.com

[illegible] © 2018 [illegible]

[illegible]

- [illegible] PKI [illegible]
- [illegible]

[illegible]

- [illegible]
  - [illegible]
  - [illegible] VPN [illegible]

[illegible] © 2018 [illegible]

HUAWEI

[illegible]

1. **[illegible]**
2. VPN [illegible]
3. VPN [illegible]

[illegible]

- [illegible]
    - [illegible]
    - [illegible]
    - [illegible] CA [illegible]

[illegible]

- [illegible]
  - VPN
  - IPv6
  - HTTPS [illegible]
  - [illegible]

[illegible]

1. [illegible]
2. **VPN [illegible]**
3. VPN [illegible]

VPN [illegible]

- [illegible] VPN(Virtual Private Network) [illegible]“[illegible] ”[illegible]
- [illegible] Internet [illegible]
- [illegible]

[illegible] © 2018 [illegible]

VPN [illegible]

SSL VPN

[illegible]

L3VPN GRE IPSec

[illegible]

L2VPN PPTP L2F L2TP

[illegible]

VPN [illegible]

- Site-to-Site VPN
  - [illegible]
  - [illegible] VPN [illegible] IPSec [illegible] L2TP [illegible] L2TP over IPSec [illegible] GRE over IPSec [illegible] IPSec over GRE [illegible]
- Client-to-Site VPN
  - [illegible]
  - [illegible] VPN [illegible] SSL [illegible] IPSec [illegible] L2TP [illegible] L2TP over IPSec [illegible]

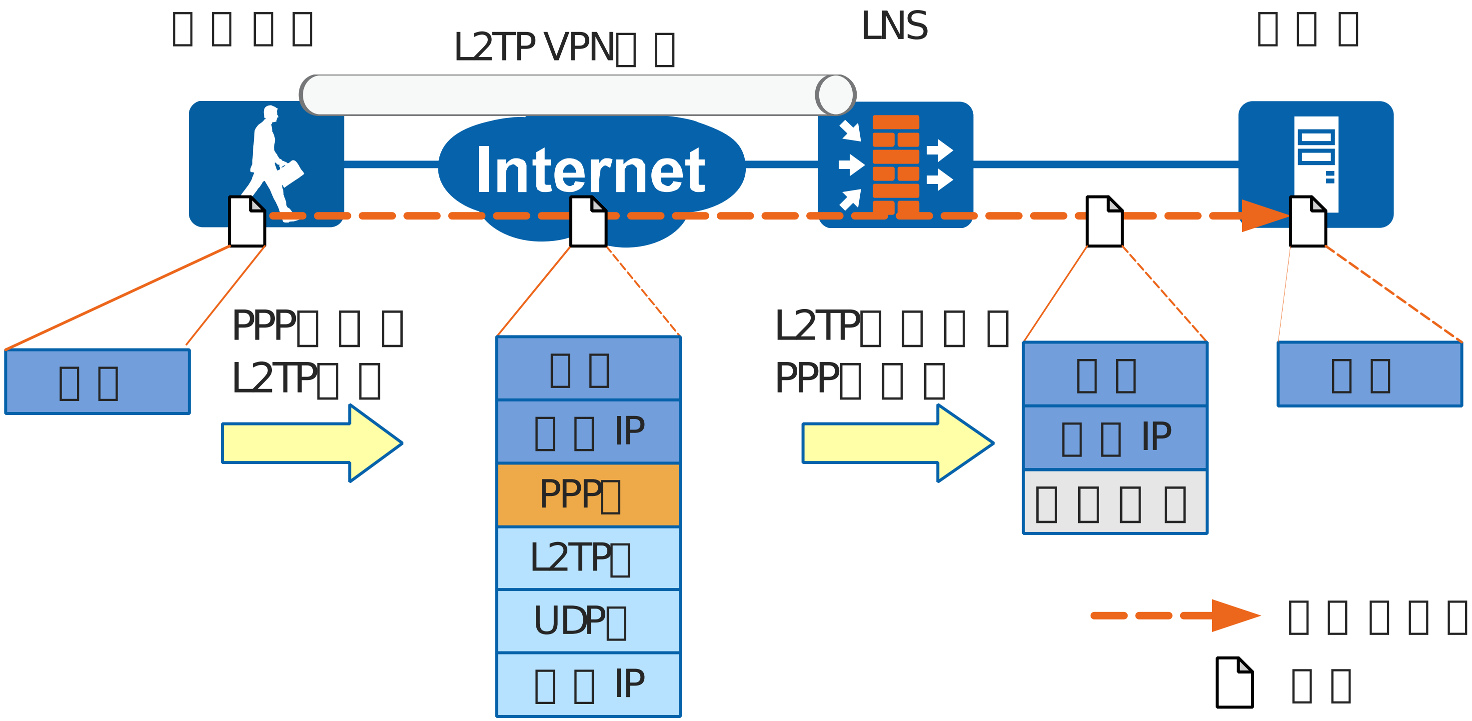
[illegible] © 2018 [illegible]

L2TP VPN [illegible]

- L2TP (Layer Two Tunneling Protocol) [illegible]
  - [illegible] PPP [illegible] PPP [illegible] Tunnel [illegible]
- L2TP VPN [illegible]
  - NAS-Initiated VPN
  - LAC [illegible]
  - Client-Initiated VPN

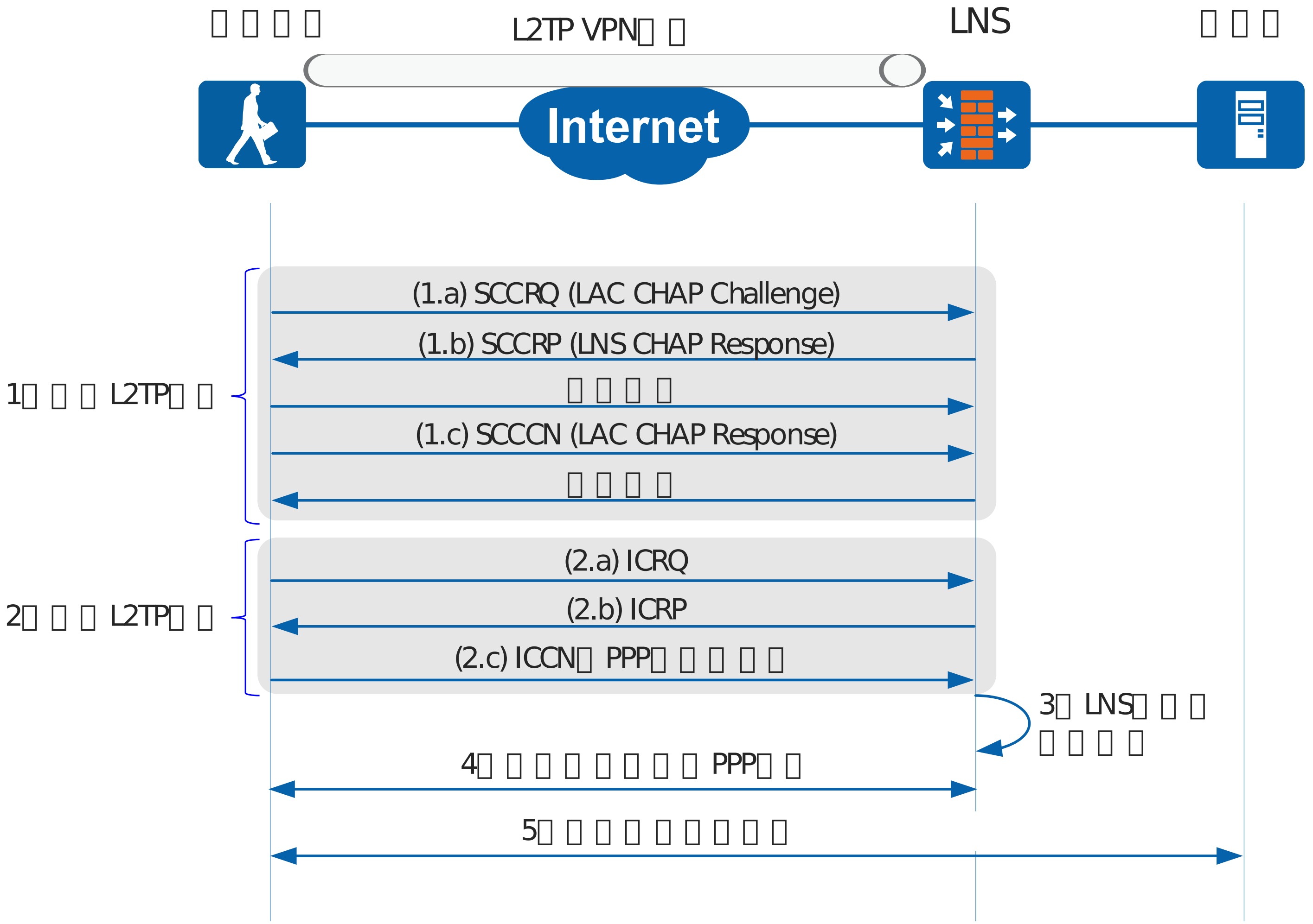
Client-Initiated VPN □□ L2TP VPN

- □□□□□□□□□□ PC □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ L2TP □□□□□



□□□□ © 2018 □□□□□□□□

Client-Initiated VPN [illegible]

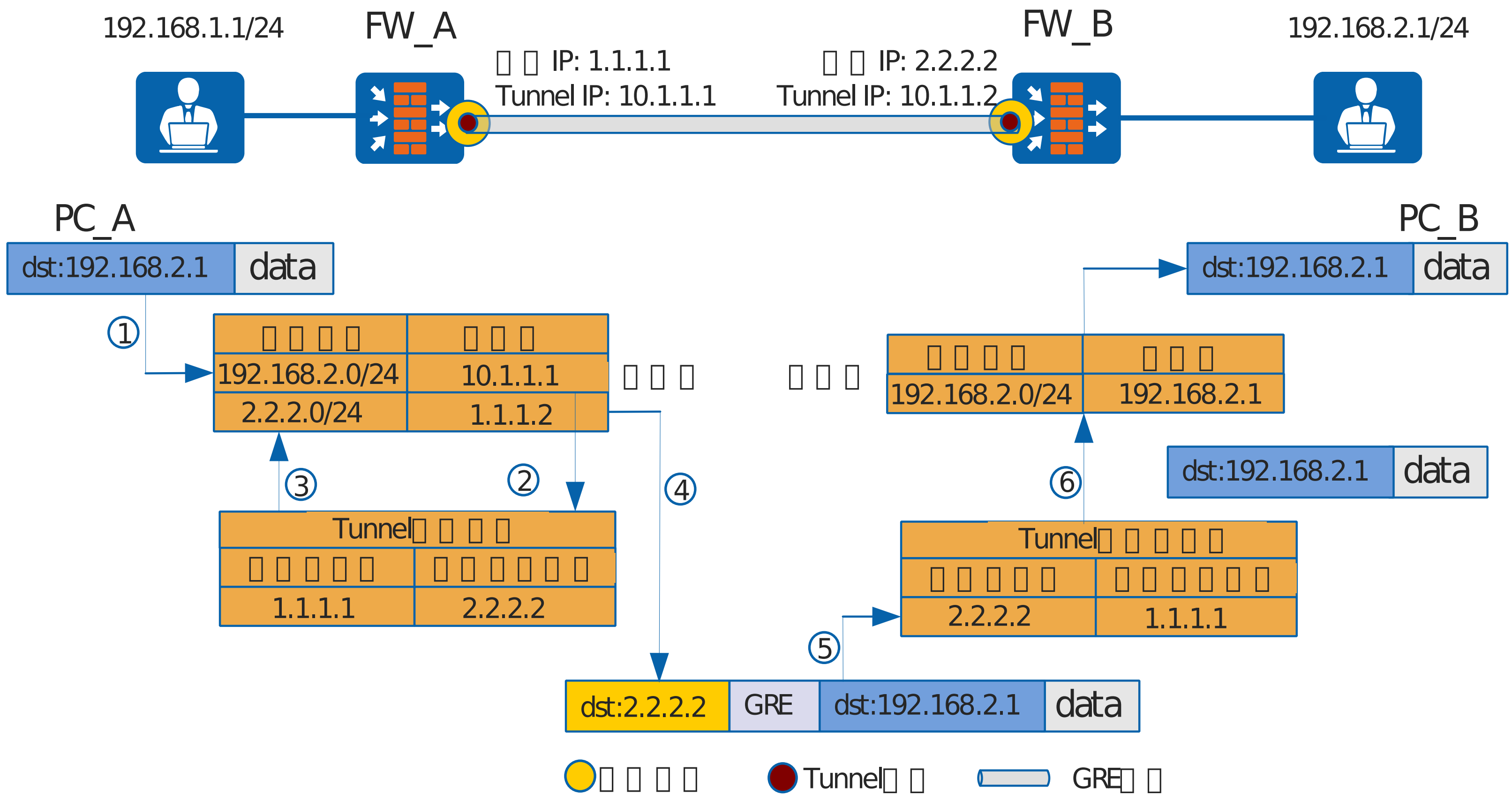


GRE VPN [illegible]

- General Routing Encapsulation [illegible] GRE [illegible] VPN [illegible] GRE [illegible] IPX [illegible] Apple Talk [illegible] IP [illegible] IPv4 [illegible] Tunnel [illegible]

[illegible] © 2018 [illegible]

GRE

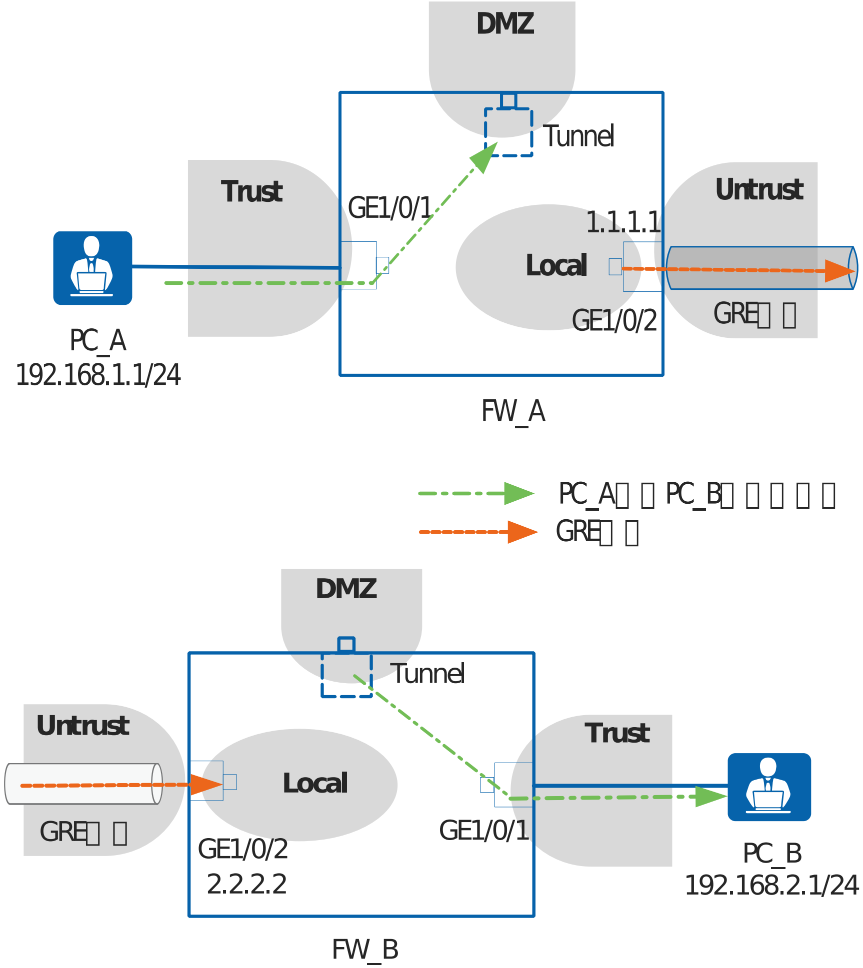


192.168.1.1/24
FW_A
IP: 1.1.1.1
Tunnel IP: 10.1.1.1
IP: 2.2.2.2
Tunnel IP: 10.1.1.2
FW_B
192.168.2.1/24
PC_A
dst:192.168.2.1
data
1
192.168.2.0/24
10.1.1.1
2.2.2.0/24
1.1.1.2
2
3
Tunnel
1.1.1.1
2.2.2.2
4
dst:2.2.2.2
GRE
dst:192.168.2.1
data
5
Tunnel
2.2.2.2
1.1.1.1
6
192.168.2.0/24
192.168.2.1
dst:192.168.2.1
data
PC_B
dst:192.168.2.1
data
Tunnel
GRE

© 2018

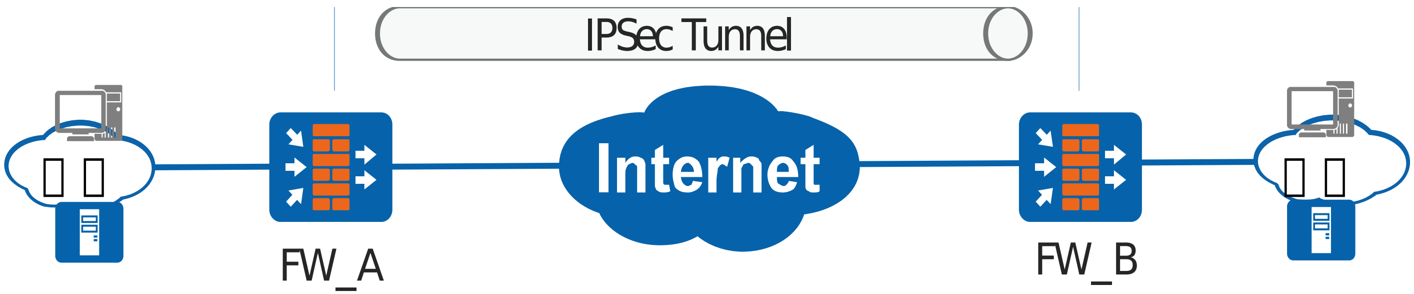
GRE □□□□

- PC_A □□□□□□□□□ Tunnel □□□□□□□□□□□□□□□□□□ Trust—>DMZ □□□□□□ GRE □□□□ FW_A □□□□□□□□□□□□□□□□□□□ Local—>Untrust
- □□□□□ FW_B □□ FW_B □□□□□□□□□□□□□□□□□□□□□□□ Untrust—>Local □ GRE □□□□□□□□ FW_B □□□□□□□□□□□□□□□□□□□ DMZ—>Trust □



IPSec VPN [illegible]

- IPSec [illegible] IP Security [illegible] IETF [illegible] IP [illegible] IPSec VPN [illegible] IPSec [illegible] VPN [illegible]



IPSec □□□□

- IPSec □□□□□ AH □ Authentication Header □□□□□□□□ ESP □ Encapsulating Security Payload □□□□□□□□□ IP □□□□□□ □□

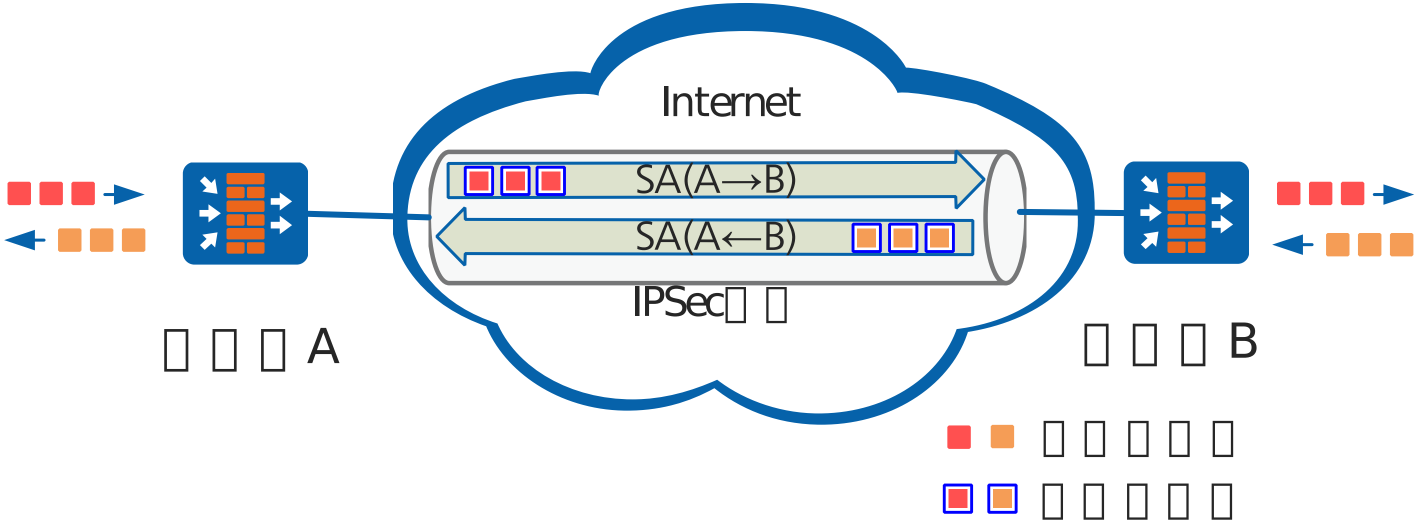
□□□□	ESP				AH			
□□	DES	3DES	AES	SM1/ SM4				
□□	MD5	SHA1	SHA2	SM3	MD5	SHA1	SHA2	SM3
□□□□	IKE□ ISAKMP□ DH□							

□□□□ © 2018 □□□□□□□□

HUAWEI

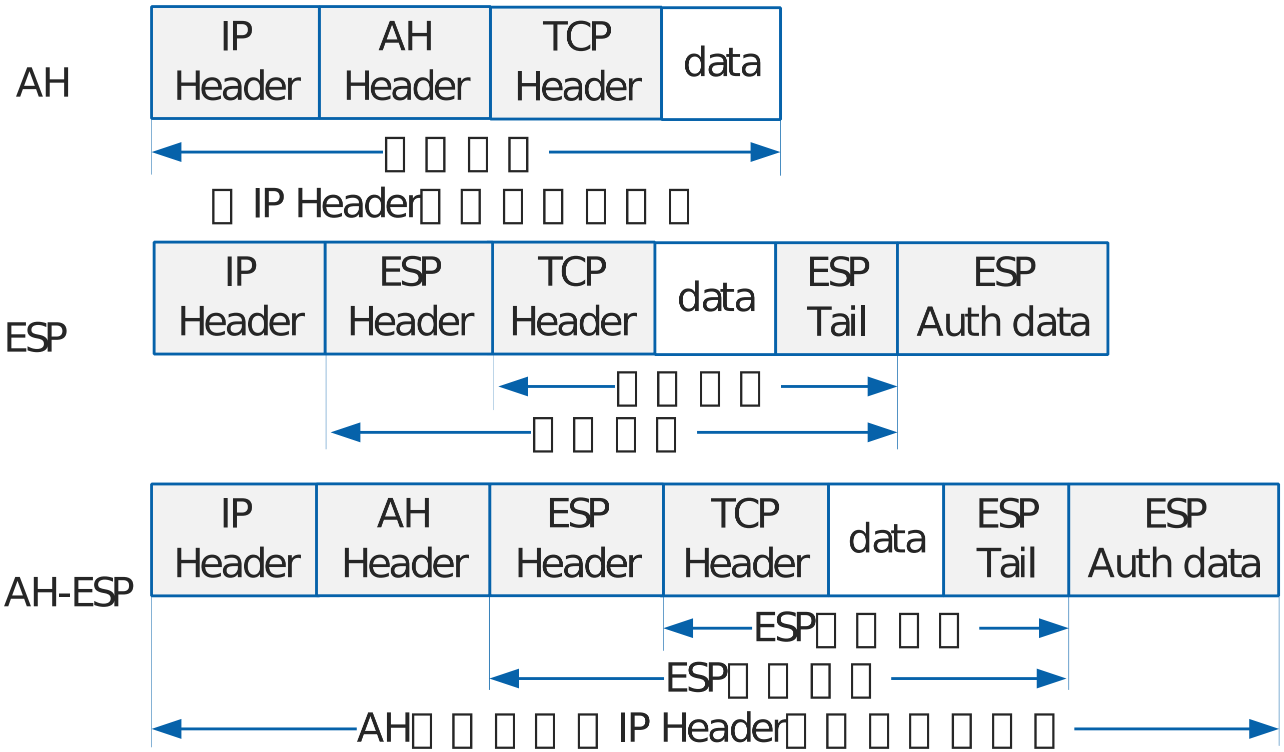
IPSec □□□□

- IPSec □□□□□□□□□□□ IPSec □□□□□□□ IPSec □□□□□□□□□□□ □□□□□□□ SA □ Security Association □□
- SA □□□□ IPSec □□□□□□□□□□□□□



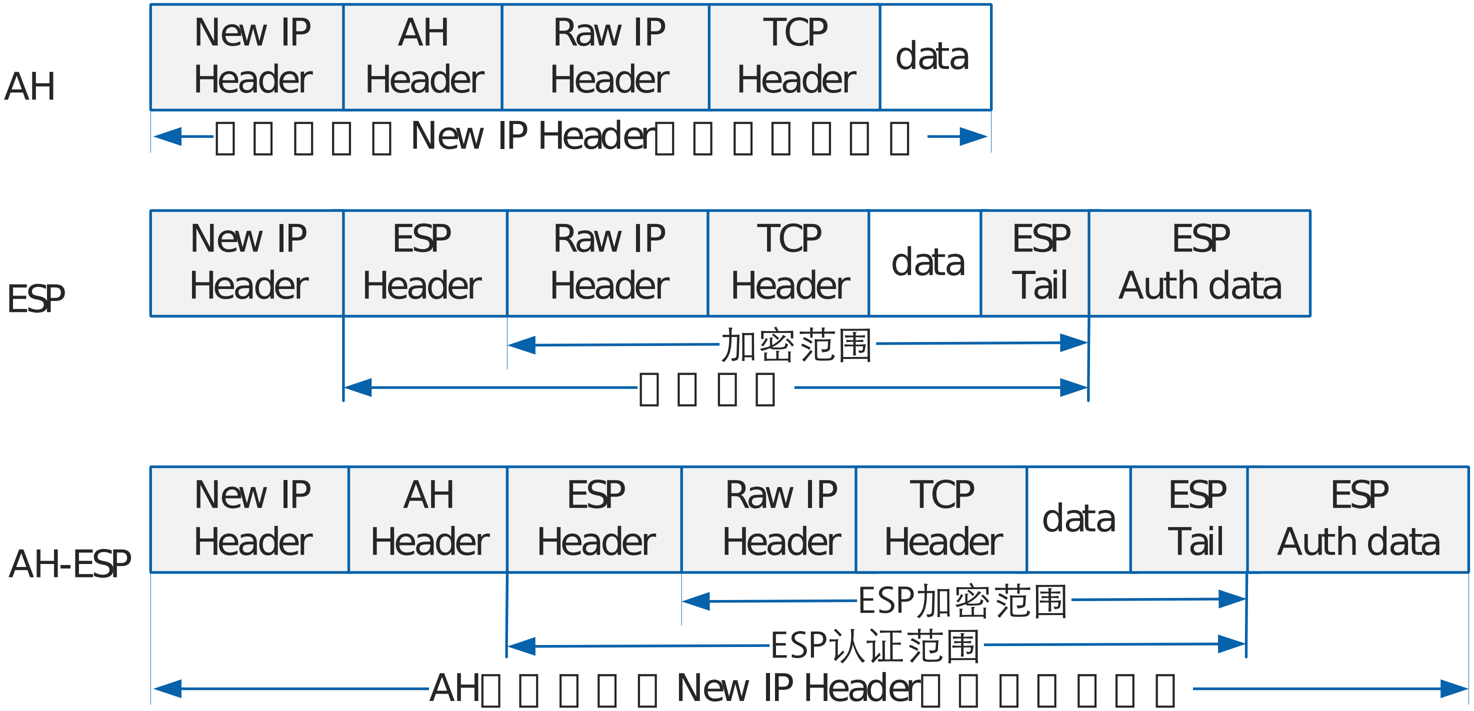
□□□□ - □□□□

- □□□□□□□ AH □□ ESP □□□□□ IP □□□□□□□□□□□□□□□□□ TCP/UDP/ICMP □□□



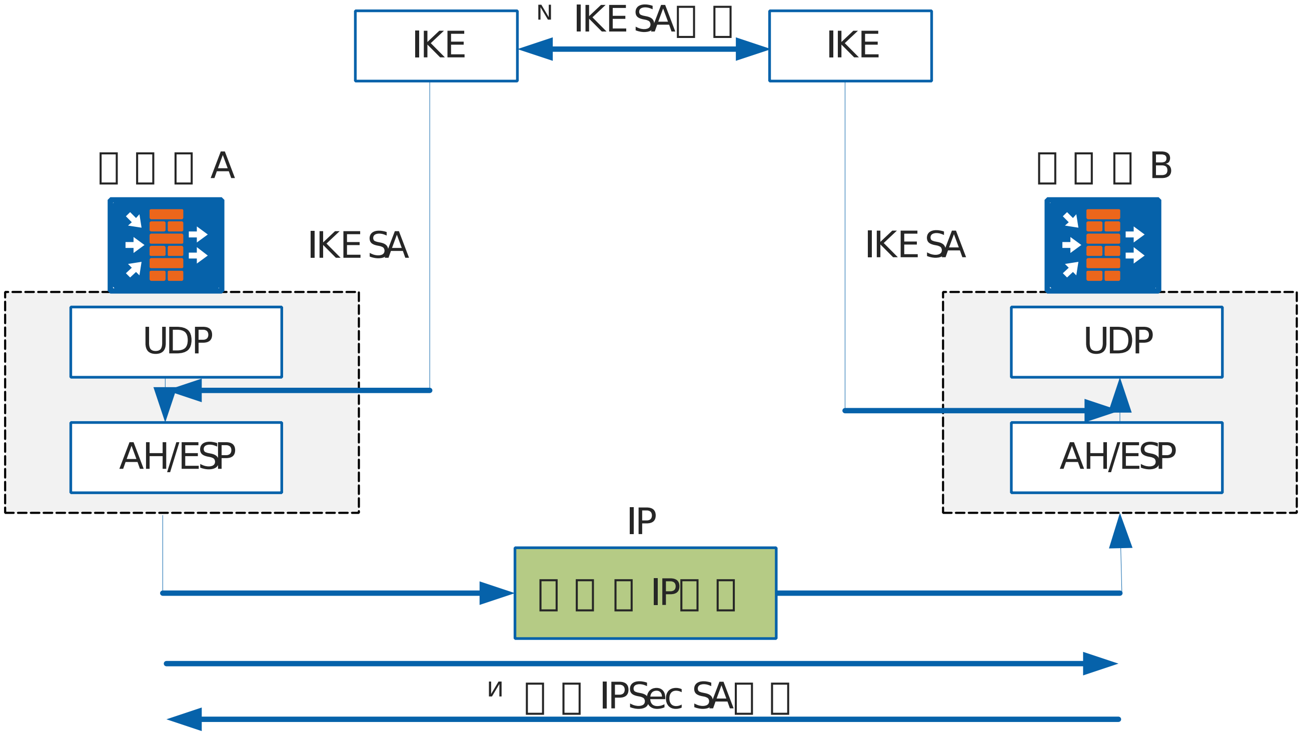
□□□□ - □□□□

- □□□□□□□AH□□ESP□□□□□□IP□□□□□□□□□□□□□□□□□□AH□□ESP□□□□□□IP□□□□□



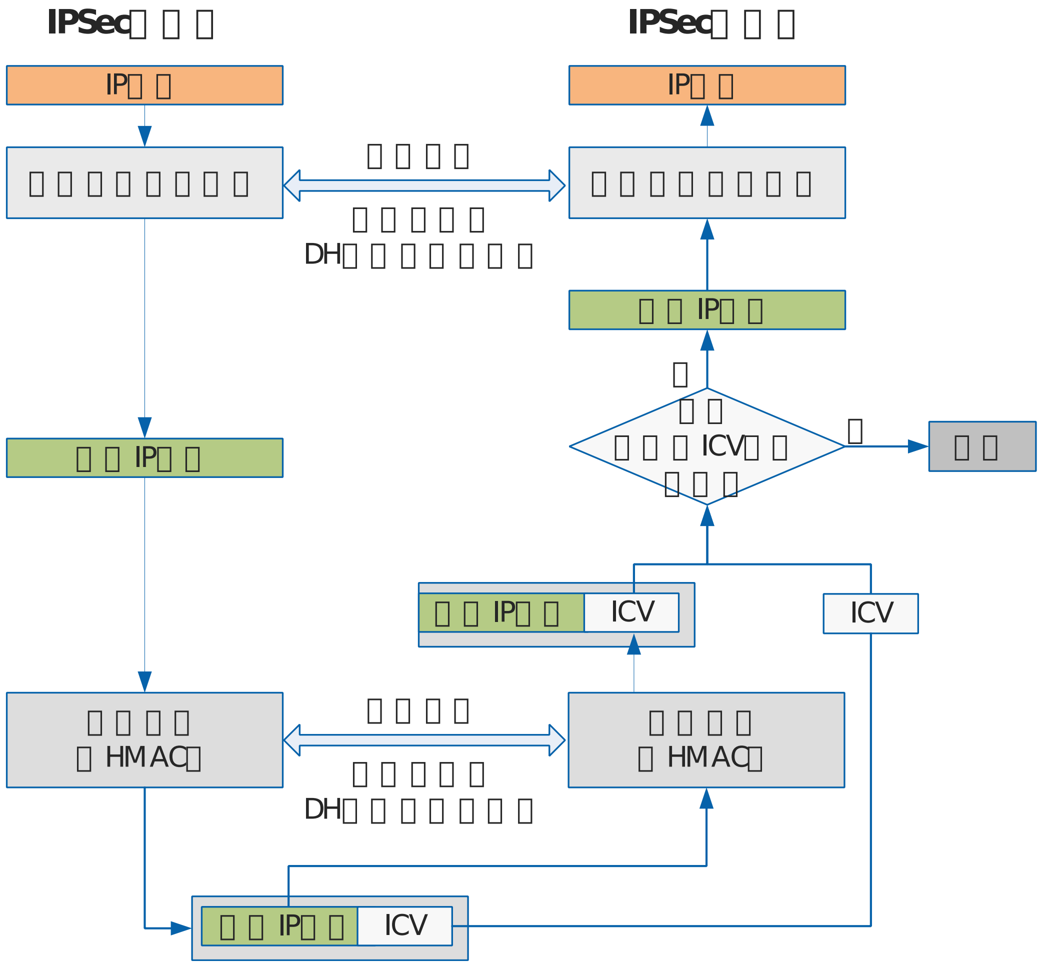
IKE SA

- IKE SA □□ IPSec SA □□□□□ IPSec □□□□□□□□□□□□ IPSec □□□□□
  □□□



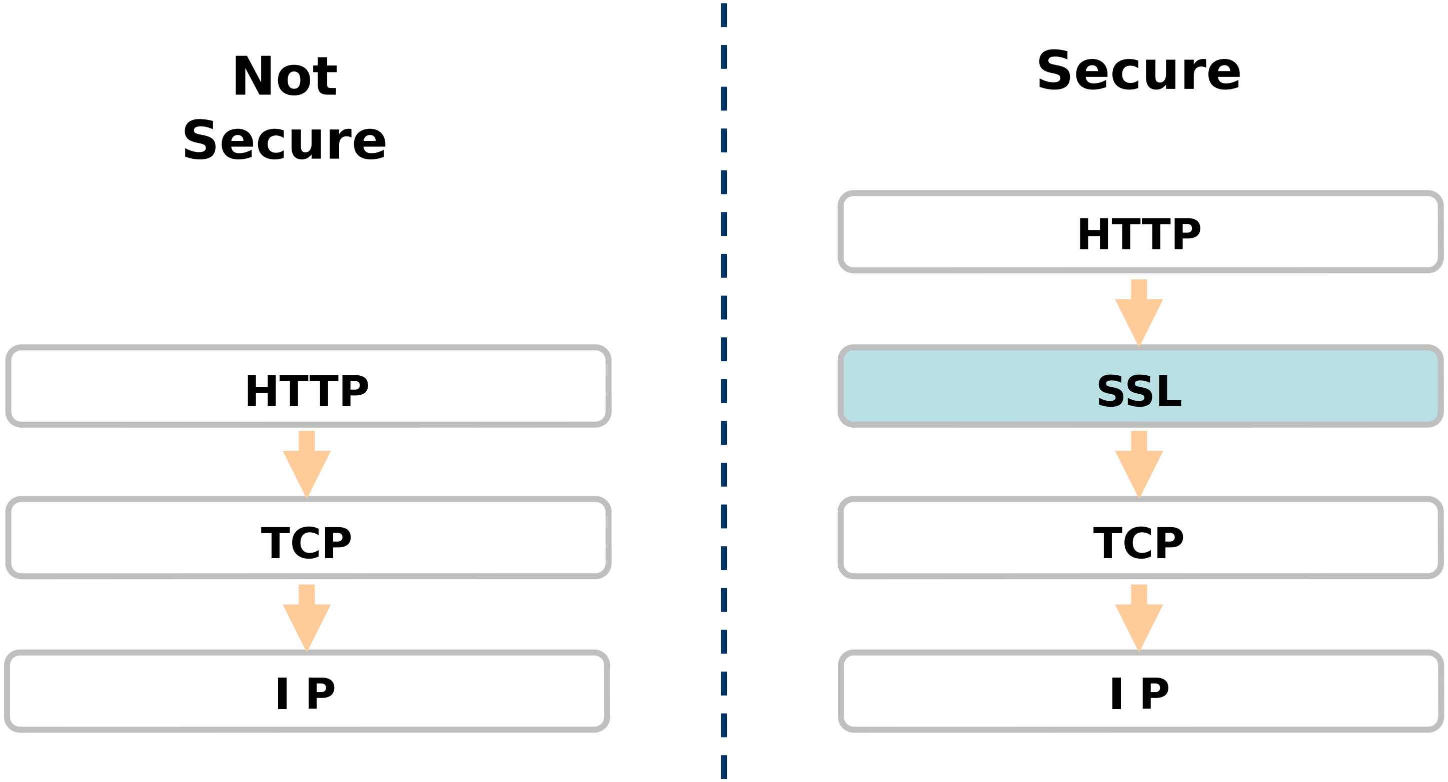
□□□□ © 2018 □□□□□□□□

IPSec [illegible]



SSL VPN [illegible]

- SSL [illegible] TCP [illegible]



SSL VPN [illegible]

SVN [illegible]

USG [illegible]

[illegible]

Web [illegible]

[illegible]

[illegible]

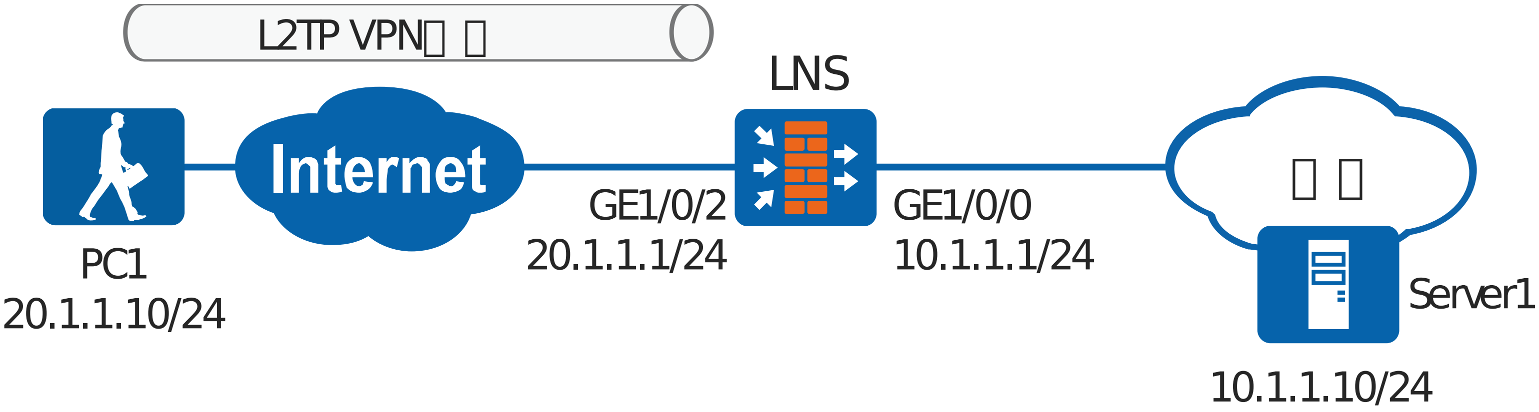
[illegible]

[illegible] © 2018 [illegible]

[illegible]

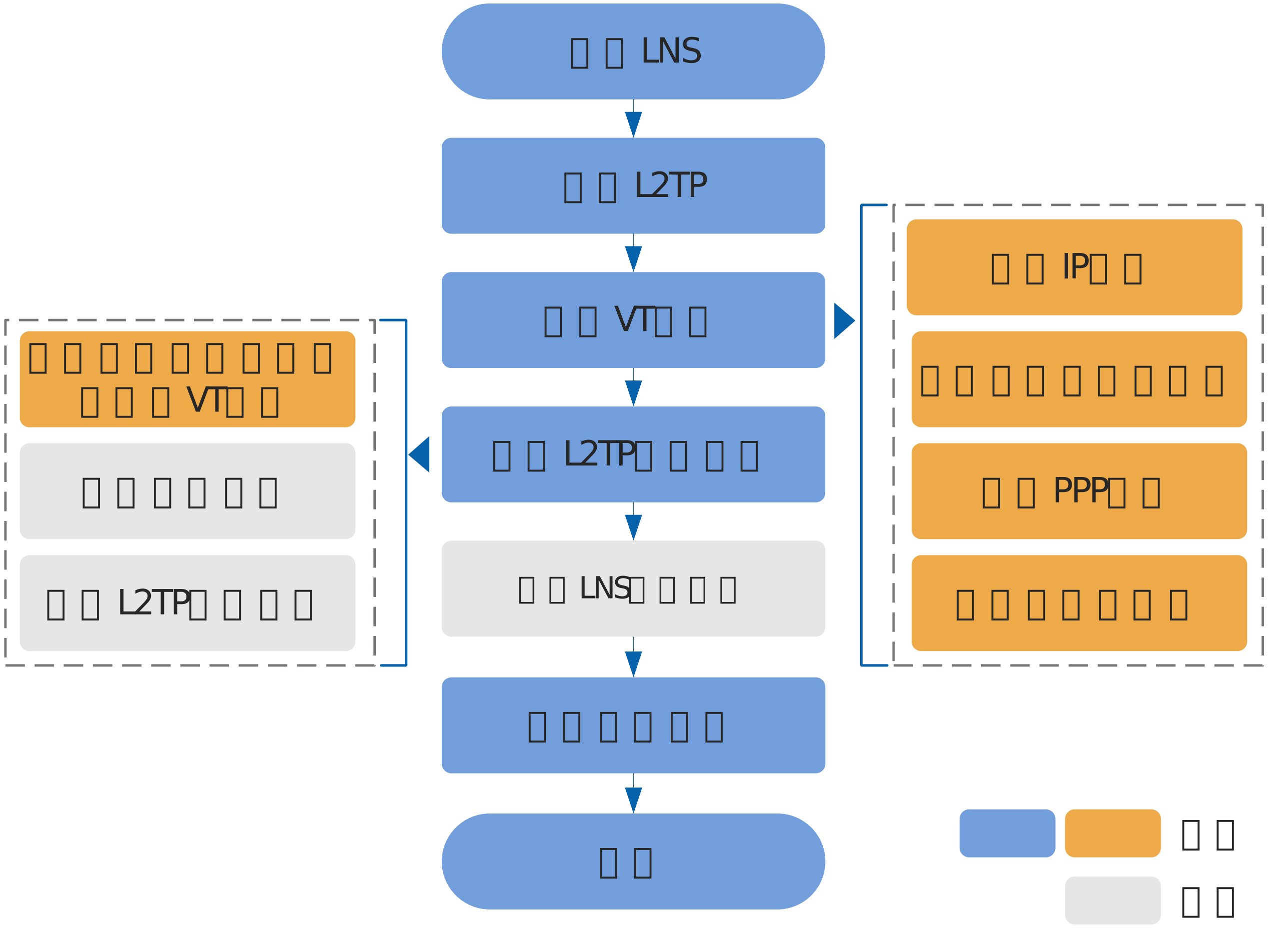
1. [illegible]
2. VPN [illegible]
3. **VPN [illegible]**

Client-Initialized [illegible] L2TP [illegible]



- [illegible]
  - [illegible] VPN [illegible] VPN [illegible] USG [illegible] L2TP [illegible]

L2TP VPN



□□ L2TP □□

- □□“□□ > L2TP > L2TP” □□“□□ L2TP” □□□□ L2TP □□“□□”□□□ “□□”□

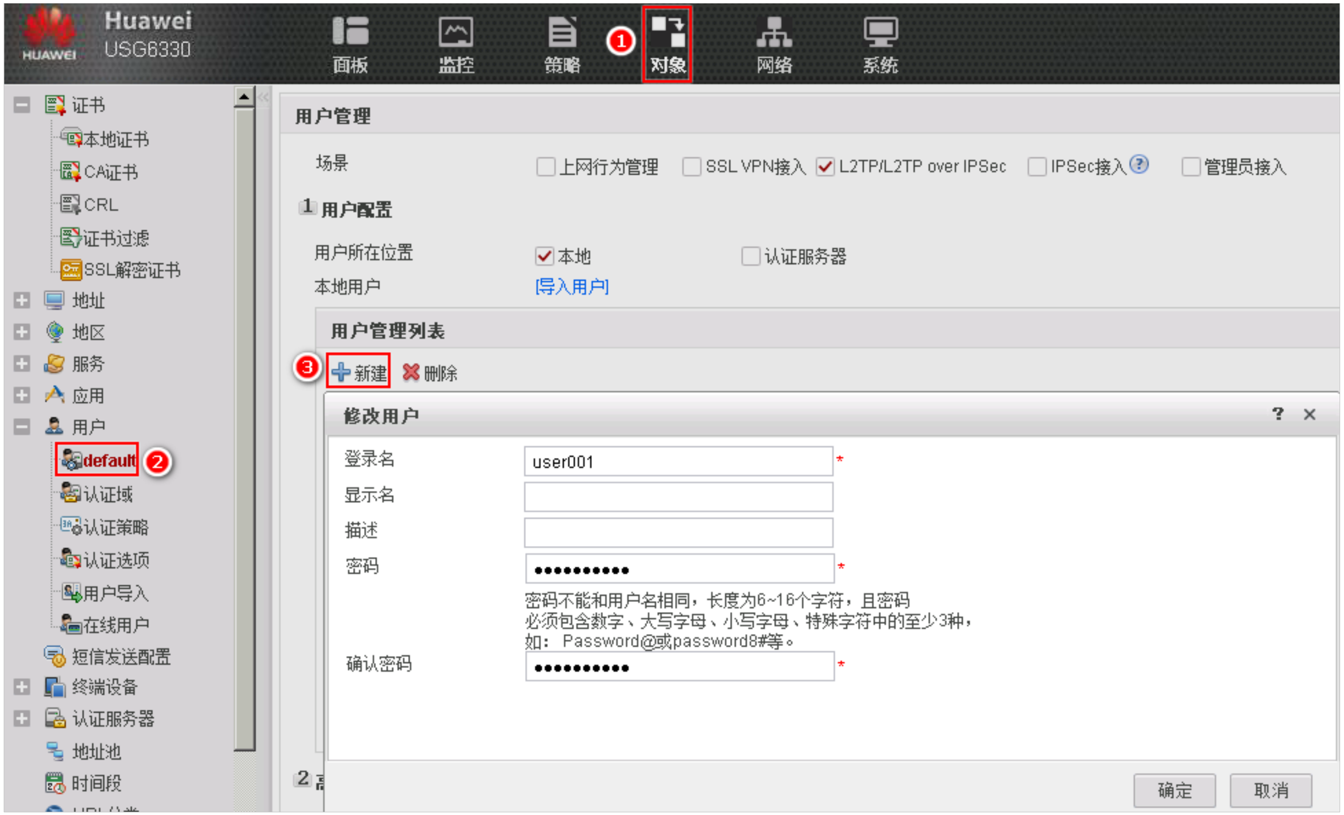
□□□□ © 2018 □□□□□□□□

[illegible] L2TP [illegible]

- [illegible]“ L2TP [illegible]”[illegible] L2TP [illegible]

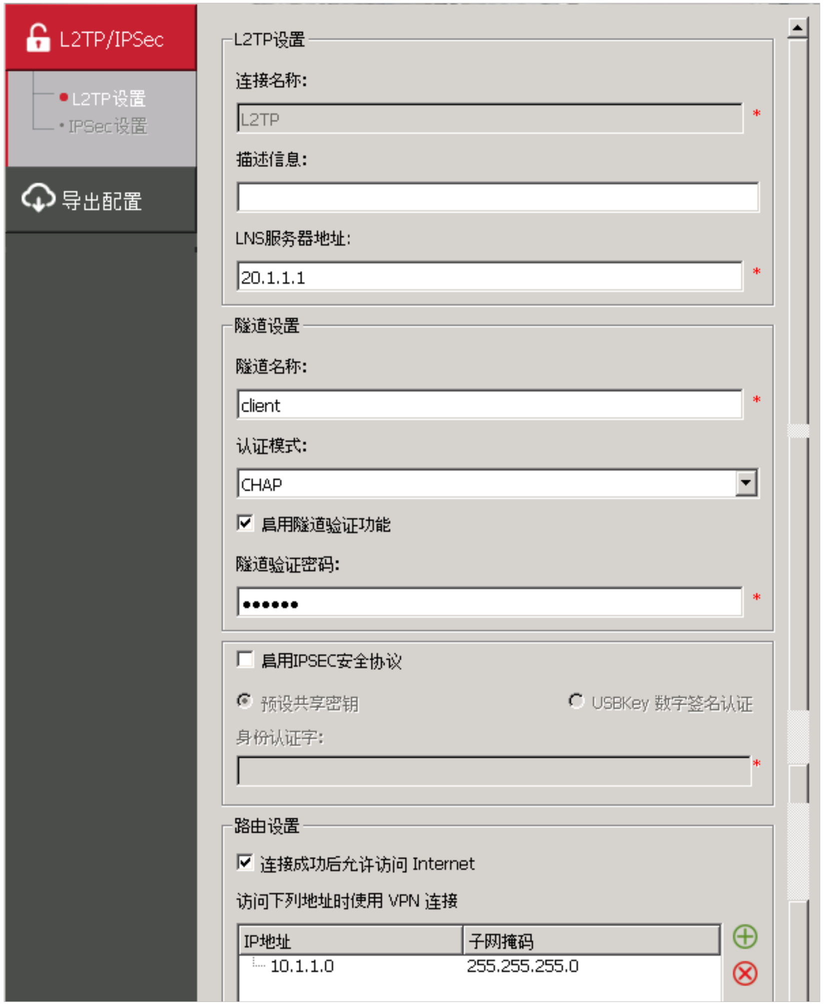
[illegible]

- [illegible]“[illegible] > [illegible]”[illegible]“ default” [illegible]“[illegible]”[illegible]“[illegible]”[illegible]“[illegible]”[illegible]



[illegible] © 2018 [illegible]

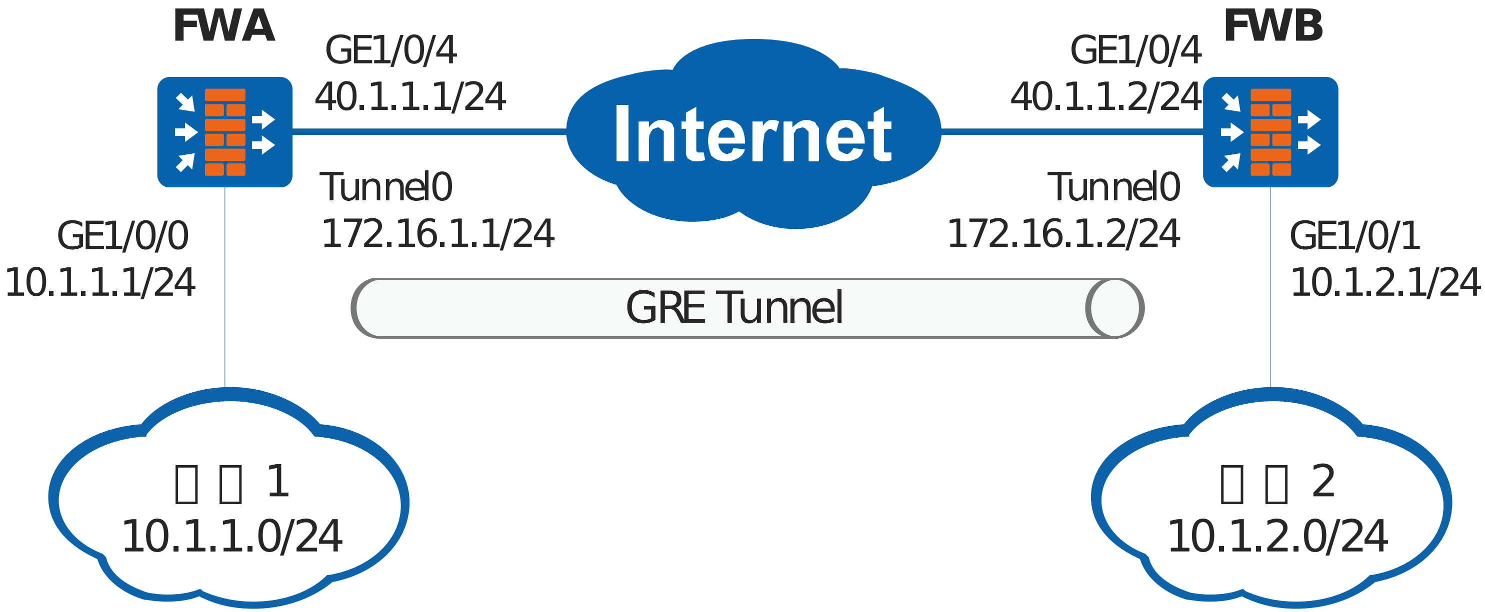
VPN □□□□□□□□


L2TP/IPSec
L2TP设置
IPSec设置
导出配置
L2TP设置
连接名称:
L2TP
描述信息:
LNS服务器地址:
20.1.1.1
隧道设置
隧道名称:
client
认证模式:
CHAP
启用隧道验证功能
隧道验证密码:
••••••
启用IPSEC安全协议
预设共享密钥
USBKey 数字签名认证
身份认证字:
路由设置
连接成功后允许访问 Internet
访问下列地址时使用 VPN 连接
IP地址
子网掩码
10.1.1.0
255.255.255.0

SecoClient
HUAWEI
登录信息
服务器地址:
20.1.1.1
用户名:
user001
密码:
••••••
记住密码
自动登录
登录

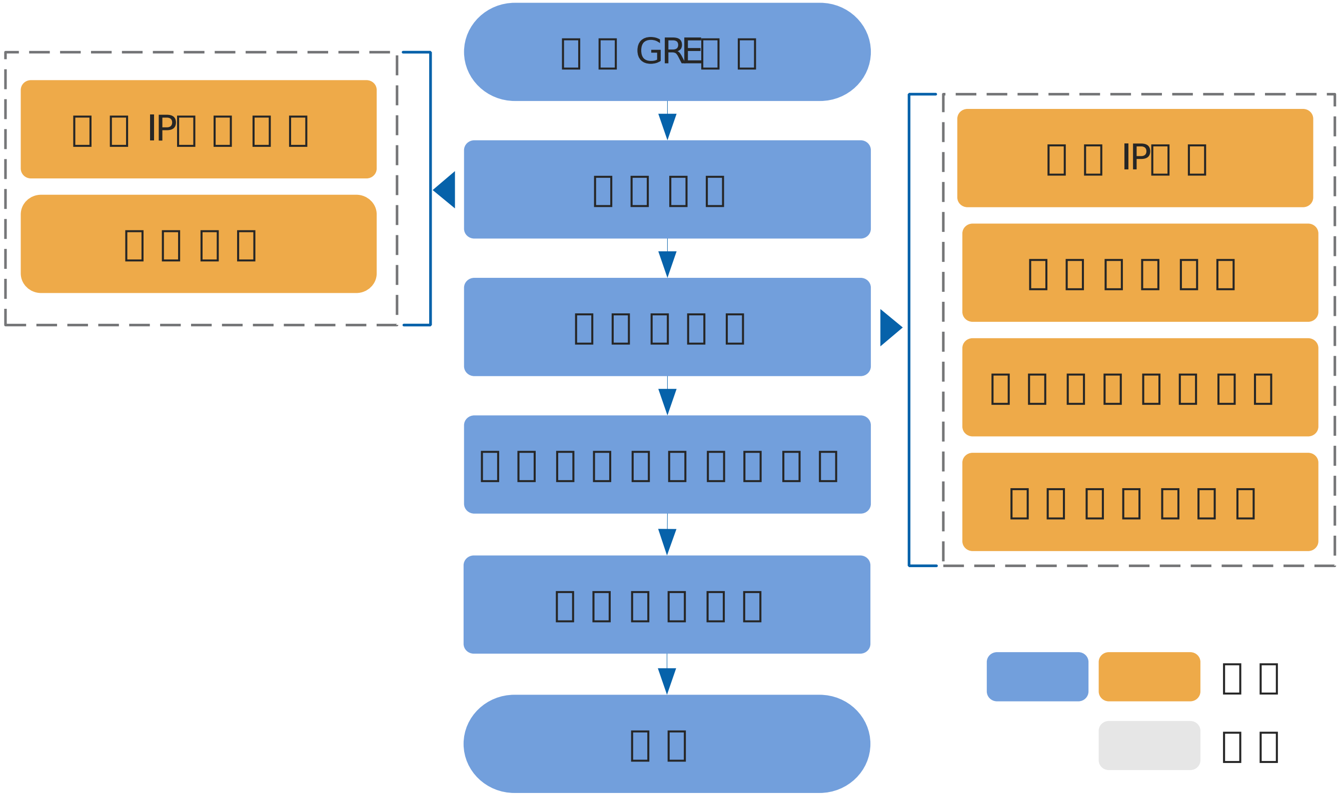
SecoClient
HUAWEI
连接:
L2TP
断开连接
代理设置

GRE □□□□□□



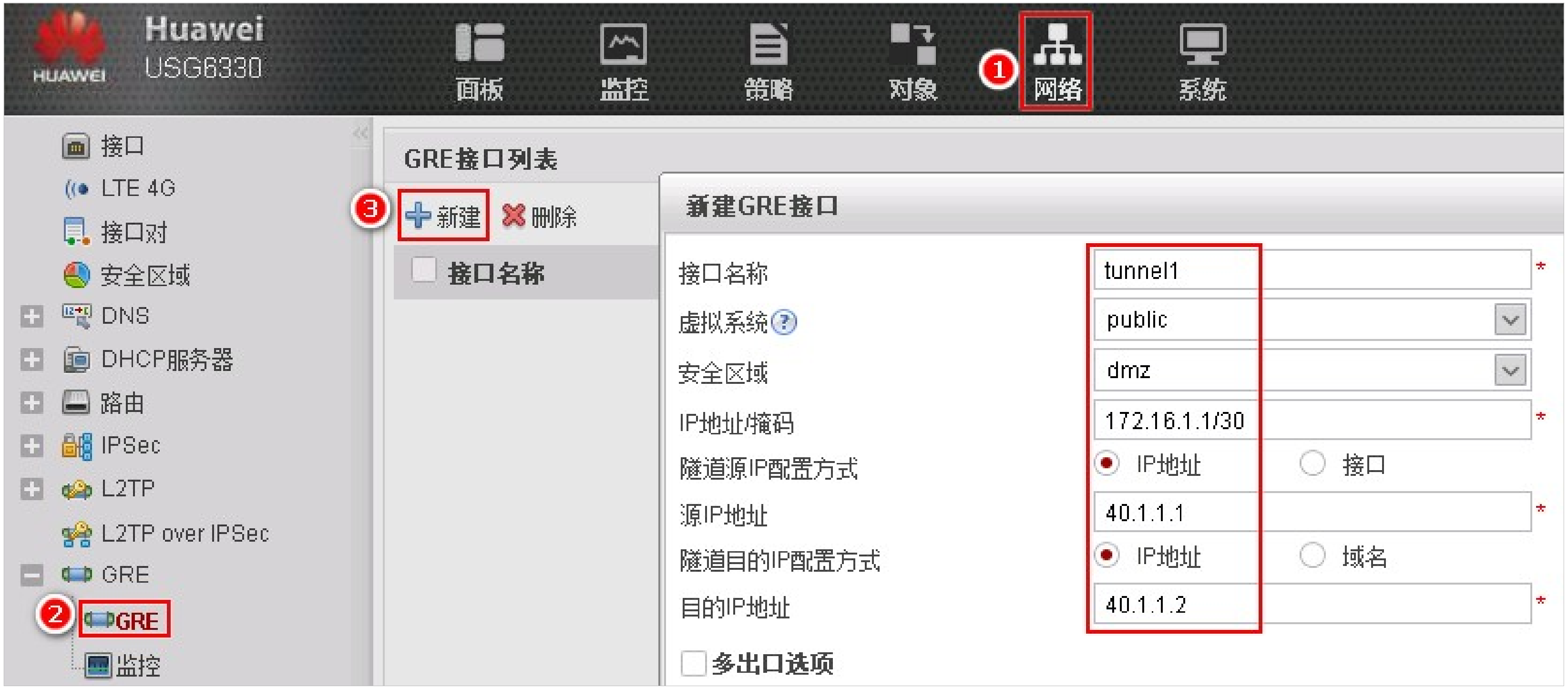
- □□□□
  - □□ IP □□□□□□□□□ 1 □□□ 2 □□□□□□□ A □□□□ B □□□□□ GRE □□□□□□□

GRE VPN



GRE □□□□ - FWA

- □□“□□ > GRE > GRE” □□□“□□”□□□ GRE □□□□□□□□□



□□□□ - FWA

- □□“□□ > □□ > □□□□”□□□“□□”，□□□□□ 2 □□□□□□

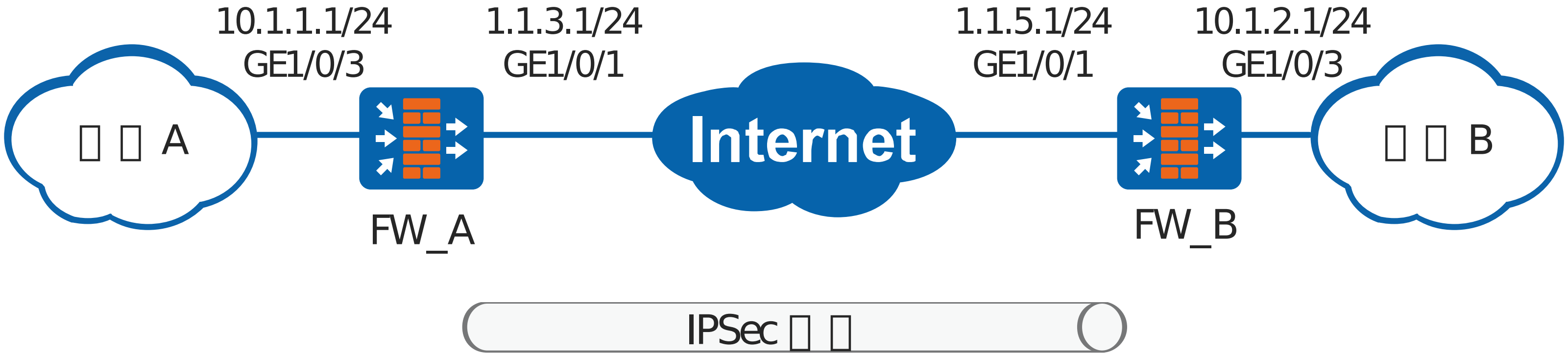
Huawei
USG6330
HUAWEI
面板
监控
策略
对象
网络
系统
接口
LTE 4G
接口对
安全区域
DNS
DHCP服务器
路由
智能选路
虚拟路由器
静态路由
配置默认优先级
IPv4默认优先级
IPv6默认优先级
静态路由列表
新建
删除
新建静态路由
协议类型
IPv4
IPv6
源虚拟路由器
public
目的地址/掩码
10.1.1.0/24
目的虚拟路由器
public
出接口
tunnel1
下一跳

□□□□

- □□1□□PC□□□2□□PC□□□□ping□□
- □□FWA“□□ > □□ > □□□”□□□□□□□□□10.1.2.0/24□□□□□Tunnel1□□□

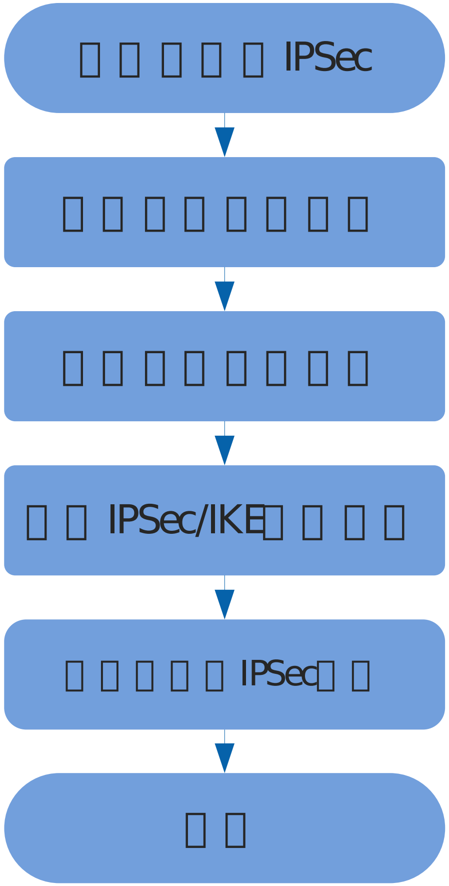
□□□□ © 2018 □□□□□□□□

□□□ IPSec VPN □□□□□□



- □□□□
  - □□ A □□□ B □□□□□ A □ B □□□□□ IPSec □□□□□□
  - IPSec □ IKE □□□□□□□□□
  - □□ IKE □□□□ IPSec □□

IPSec VPN



□□□□

- □□□□□□□□□□□□□ FW_A □□□□□□□□□□□ FW_B □□□□□

Huawei
USG6330
面板
监控
策略
对象
网络
系统
接口
LTE 4G
接口对
安全区域
VXLAN
DNS
DHCP服务器
路由
智能选路
虚拟路由器
静态路由
RIP
配置默认优先级
IPv4默认优先级
IPv6默认优先级
静态路由列表
新建
删除
源虚拟路由器
新建静态路由
协议类型
IPv4
IPv6
源虚拟路由器
public
目的地址/掩码
10.1.2.0/24
目的虚拟路由器
public
出接口
-- NONE --
下一跳
40.1.1.2
优先级
60
可靠性检测
不检测
绑定BFD
描述

□□□□ © 2018 □□□□□□□□

□□□□□□

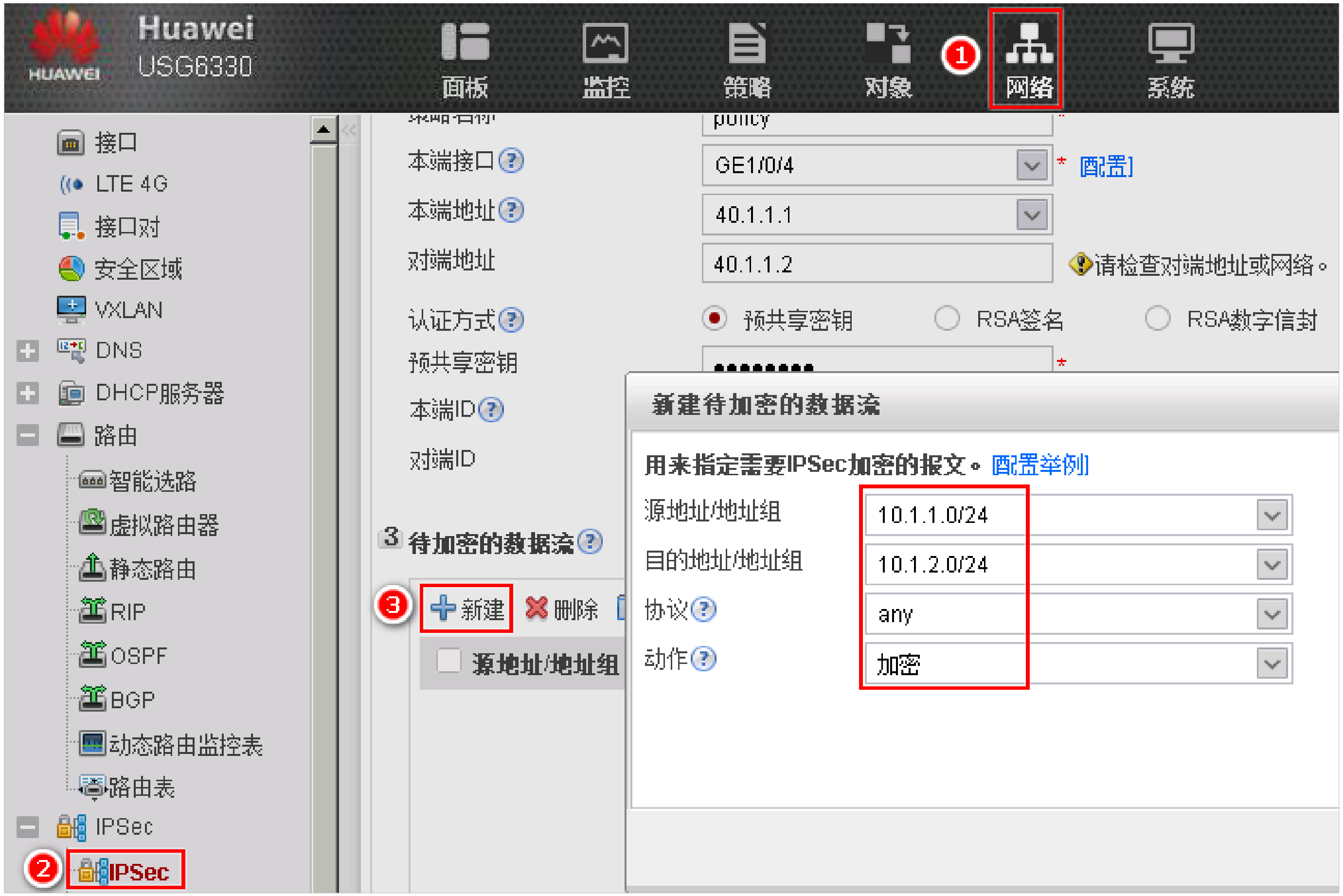
IPSec		FW_A	FW_B
□□□□A□□□B□□	ipsec 1	□□□trsut > untrust □□□□10.1.1.0/24 □□□□□10.1.2.0/24 □□□□□	□□□trsut > untrust □□□□10.1.2.0/24 □□□□□10.1.1.0/24 □□□□□
	ipsec 2	□□□untrsut > trust □□□□10.1.2.0/24 □□□□□10.1.1.0/24 □□□□□	□□□untrsut > trust □□□□10.1.1.0/24 □□□□□10.1.2.0/24 □□□□□
□□IKE□□□□□□	ipsec 3	□□□local > untrust □□□□40.1.1.1/24 □□□□□40.1.1.2/24 □□□□□	□□□local > untrust □□□□40.1.1.2/24 □□□□□40.1.1.1/24 □□□□□
	ipsec 4	□□□untrust > local □□□□40.1.1.2/24 □□□□□40.1.1.1/24 □□□□□	□□□untrust > local □□□□40.1.1.1/24 □□□□□40.1.1.2/24 □□□□□

□□□□© 2018 □□□□□□□□

IPSec □□□□□□ - FW_A

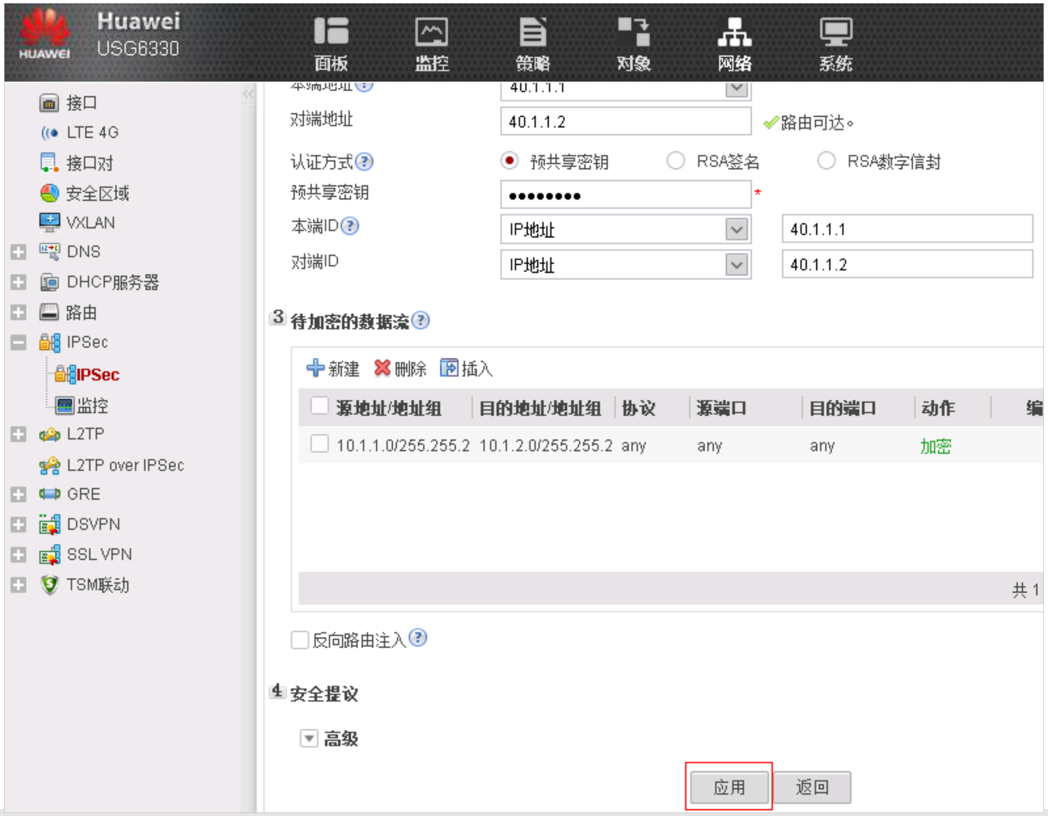
□□□□ © 2018 □□□□□□□□

□□□□□□□


Huawei
USG6330
HUAWEI
面板
监控
策略
对象
1
网络
系统
接口
LTE 4G
接口对
安全区域
VXLAN
DNS
DHCP服务器
路由
智能选路
虚拟路由器
静态路由
RIP
OSPF
BGP
动态路由监控表
路由表
IPSec
2
IPSec
policy
本端接口
GE1/0/4
[配置]
本端地址
40.1.1.1
对端地址
40.1.1.2
请检查对端地址或网络。
认证方式
预共享密钥
RSA签名
RSA数字信封
预共享密钥
本端ID
对端ID
3 待加密的数据流
3
新建
删除
源地址/地址组
新建待加密的数据流
用来指定需要IPSec加密的报文。
配置举例
源地址/地址组
10.1.1.0/24
目的地址/地址组
10.1.2.0/24
协议
any
动作
加密

□□ IPSec □□

- □□□□□□□□□□□□□□□“□□”□□□□□□ IPSec □□□



Huawei
USG6330
HUAWEI
面板
监控
策略
对象
网络
系统
接口
LTE 4G
接口对
安全区域
VXLAN
DNS
DHCP服务器
路由
IPSec
IPSec
监控
L2TP
L2TP over IPSec
GRE
DSVPN
SSL VPN
TSM联动
对端地址
40.1.1.2
路由可达。
认证方式
预共享密钥
RSA签名
RSA数字信封
预共享密钥
••••••••
本端ID
IP地址
40.1.1.1
对端ID
IP地址
40.1.1.2
3 待加密的数据流
新建
删除
插入
源地址/地址组
目的地址/地址组
协议
源端口
目的端口
动作
10.1.1.0/255.255.2
10.1.2.0/255.255.2
any
any
any
加密
共 1
反向路由注入
4 安全提议
高级
应用
返回

[illegible]

1. [illegible] IPSec [illegible] （ ）
   - A. [illegible]
   - B. [illegible]
2. [illegible] USG6000 [illegible] SSL VPN [illegible] （ ）
   - A. [illegible]
   - B. [illegible]
   - C. [illegible]
   - D. Web [illegible]

[illegible]

- [illegible]
- VPN [illegible]
- GRE VPN [illegible] L2TP VPN [illegible]
- IPSec VPN [illegible]
- [illegible] VPN [illegible]

[illegible] © 2018 [illegible]

[illegible]

www.huawei.com